Towards Trust-aware Automotive Task-offloading

Vasilis Milionis
ICCS
Athens, Greece
vasilis.milionis@iccs.gr

Stefanos Vasileiadis
Ubitech Ltd.
Athens,Greece
svasileiadis@ubitech.eu

Pavlos Basaras
ICCS
Athens, Greece
pavlos.basaras@iccs.gr

Panagiotis Pantazopoulos
ICCS
Athens, Greece
ppantaz@iccs.gr

Thanassis Giannetsos
Ubitech Ltd.
Athens, Greece
agiannetsos@ubitech.eu

***Abstract*—Shifting tasks from low-capability in-vehicle processing units to the powerful (edge) infrastructure has lately been considered as a promising means to offload non safety-critical tasks from the vehicles fleet computational load. Still, research so far has hardly addressed (and experimentally explored) the way to effectively converge the networking mechanisms with distributed trust-anchoring capabilities; this combination is mostly needed in view of the emerging yet trustworthiness-demanding, connected vehicles paradigm. The CONNECT EU project implements and evaluates through an automotive video-analytics service, the efficiency of networking and trusted-computing mechanisms to realize the *trust-aware* task offloading vision. To that end, our modeling and on-going experiments will be discussed in-depth.**

***Index Terms*—Task-offloading, Trusted computing, MEC**

I. Introduction

The CONNECT EU project [1], adopting a zero-trust hypothesis, introduces a trust management framework to assess the automotive dynamic trust relations among entities without central authority. A significant part of the considered research relates to the way task-offloading operations can rely on trust relations. The offloading challenge, driven by increased in-vehicle computation needs (due to higher vehicle levels, requiring advanced ML-based, cooperative perception and positioning capabilities [2]) can be defined as follows [3]: *efficient transferring of a (part of a) resource intensive computational task from a resource-limited end-device to an appropriate location in the resource-rich infrastructure (i.e., Multi-Access Edge Computing (MEC)), under given network conditions*. While the above definition bears exploration along a number of dimensions (e.g., splitting of tasks, placement across MEC facilities or PDI resource allocation), it is the trust considerations [4] that have been largely under-explored.

To establish trustworthiness in the involved PDI, CONNECT requires for a trust relation to have been established between the two sides. Trustworthiness in this context goes beyond the current heavy reliance on data integrity and also considers other core trust properties on safety, resileince, availability, robustness, etc. Pivotal constructs underpinning interactions between all elements, in a continuously changing environment, based on the secure and privacy-preserving extraction of (verifiable) evidence. This necessitates the appropriate definition of the security structures (realised in a trusted computing base - see Fig. 1) that can hold this information.

II. Design, Implementation and Expected Results

Assuming a distributed cluster of containerized applications managed by appropriate software [5], our main challenge involves the design, extraction and appropriate reasoning (trust assessment framework) of the required information to ensure that offloading tasks is trustworthy. We consider an ML-based video analytics application which offloads data captured by vehicle sensors to the MEC for inference. We introduce the CONNECT Trusted Computing Base (see Fig. 1) which

- can self-issue verifiable statements [6] to ensure that an entity exhibits a certain attribute;
- employs TEEs (where evidence is collected) and key establishment mechanisms to realize distributed Roots-of-Trust (for CCAM);
- introduces a dynamic trust assessment framework [7];

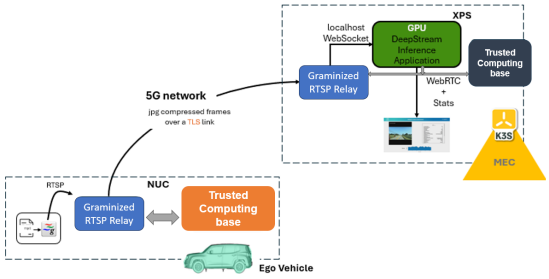

Fig. 1. The CONNECT architectural design for trusted offloading

Our modeling, implementation and on-going testing results will be presented to highlight the trust dimension in PDI.

Acknowledgment

This research has received funding from the European Union's Horizon EU CONNECT Research & Innovation program under Grant Agreement No 101069688.

References

[1] Horizon CONNECT project: Continuous and Efficient Cooperative Trust Management for Resilient CCAM, https://horizon-connect.eu/.

[2] Aaron Miller et al., "Cooperative perception and localization for cooperative driving", In 2020 IEEE ICRA, pp 1256–1262, 2020.

[3] CONNECT Public deliverable D5.1 "Distributed Processing and CCAM Trust Functions Offloading & Data Space Modelling", https://horizon-connect.eu/public-deliverables/.

[4] Dexiang Wu et al., "A trust-aware task offloading framework in mobile edge computing". IEEE Access, 7:150105–150119, 2019.

[5] Lightweight Kubernetes distribution https://k3s.io/

[6] Oliver Terbu et al., "Verifiable credentials data model v2.0". W3C working draft, August 2024. https://www.w3.org/TR/vc-data-model-2.0/.

[7] CONNECT Public deliverable D3.1 "Architectural Specification of CONNECT Trust Assessment Framework" https://horizon-connect.eu/wp-content/uploads/2024/04/CONNECT-D3.1-PU-M10.pdf